

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH CELL PHONE  
ACCOUNT 215-390-7572, IMSI # 310260152840513

Case No. 18- *1756-M-1*

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A hereto

located in the \_\_\_\_\_ District of \_\_\_\_\_ New Jersey \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 USC Section 1001

Offense Description  
False Statements

The application is based on these facts:

See the attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Joseph W. O'Connor*

Applicant's signature

Joseph W. O'Connor, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/1/2018

*L. K. Caracappa*

Judge's signature

City and state: Philadelphia, PA

Hon. Linda K. Caracappa, Chief United States Magistrate Judge

Printed name and title

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH CELL PHONE  
ACCOUNT 513-283-3799, IMSI # 310120155694040

Case No. 18- 1756-M-2

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment C hereto

located in the \_\_\_\_\_ District of Kansas, there is now concealed (identify the person or describe the property to be seized):

See Attachment D hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 USC Section 1001

Offense Description  
False Statements

The application is based on these facts:

See the attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Joseph W. O'Connor, Special Agent  
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/1/2018

City and state: Philadelphia, PA

  
Judge's signature

Hon. Linda K. Caracappa, Chief United States Magistrate Judge  
Printed name and title



**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
CELL PHONE ACCOUNT **215-390-7572**,  
THAT IS STORED AT PREMISES  
CONTROLLED BY T-MOBILE USA, INC  
AND THE CELL PHONE ACCOUNT **513-  
283-3799**, THAT IS STORED AT  
PREMISES CONTROLLED BY SPRINT  
PCS.

Case No. 18-1756-M

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Joseph W. O'Connor, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require T-Mobile USA, Inc. to disclose to the government records and other information associated with the below-listed T-Mobile USA, Inc. cellular telephone account for cellular telephone number **215-390-7572**, IMSI:

310260152840513, used by Daniel Denmark, 620 Anchor Street, Philadelphia Pa 19120, from March 1, 2018 to present, that is stored at premises owned, maintained, controlled, or operated by T-Mobile USA, Inc., 4 Sylvan Way, Parsippany, New Jersey, 07054. The information to be disclosed by T-Mobile USA, Inc. and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I also make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Sprint PCS to disclose to the

government records and other information associated with the below-listed Sprint PCS cellular telephone account for cellular telephone number **513-283-3799**, IMSI: 310120155694040, used by Melanie Newman, and subscribed to Anthony Newman, 3119 Westmont Street, Philadelphia Pa 19121, from March 1, 2018 to present, that is stored at premises owned, maintained, controlled, or operated by Sprint PCS, 6480 Sprint Parkway, Overland Park, KS 66251. The information to be disclosed by Sprint PCS and searched by the government is described in the following paragraphs and in Attachments C and D.

3. I have been a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”) since May 2017. I am currently assigned to the FBI White Collar Crimes Branch in Philadelphia, Pennsylvania, whose mission includes the investigation of crimes involving law enforcement corruption. During that time, I have been involved in investigating violations of civil rights, fraud against the government, and public corruption. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses. Moreover, I am a licensed certified public accountant (“CPA”) in Pennsylvania. I am aware that individuals engaged in criminal activity commonly use mobile phones in furtherance of their illegal activity. I am also aware that such individuals often speak and text in vague, guarded, or coded language when discussing their illegal activities – especially over telephones – in an effort to prevent detection.

4. The information contained in this affidavit is known to me personally or has been relayed to me by other law enforcement officers or other individuals assisting law enforcement officers, as indicated below. Because this affidavit is being submitted for the limited purpose of establishing that there is sufficient probable cause for the requested warrant, I have not included



every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the information from T-Mobile USA, Inc. and Sprint PCS – as set forth in Attachments A and C – contain evidence, instrumentalities, and fruits of criminal violations of 18 U.S.C. § 1001(a)(2) (makes any materially false, fictitious, or fraudulent statement or representation). I further respectfully submit that probable cause exists to search the information described in Attachments A and C for evidence of these crimes as described in Attachments B and D.

#### **PROBABLE CAUSE**

6. I have participated in the investigation of the offenses described below since May 2018. This is a joint investigation being worked cooperatively with the FBI and the Philadelphia Department of Prisons (“PDP”). As a result of my personal participation in the investigation, through interviews, and analysis of phone records, I allege the facts enumerated below to show that:

7. There is probable cause to believe that: DANIEL DENMARK and MELANIE NEWMAN, have committed the following offenses: which are enumerated in Title 18, United States Code, Section 2516:

- i. False statements, in violation of Title 18, United States Code, Section 1001(a)(2);

8. On May 2, 2018, Lt. Joseph Fanelli, Internal Affairs, PDP and Corrections Officer (“CO”) DANIEL DENMARK, PDP had a three way phone call with Your Affiant, in which

DENMARK stated that he had found narcotics on the bathroom sink in the home of fellow a CO, MELANIE NEWMAN, on April 26, 2018 and reported the incident to Deputy Commissioner Clark, PDP on April 30, 2018. DENMARK believed the packages of narcotics to look the same as those found in a recent search of a cell at Philadelphia Industrial Correctional Center ("PICC") and that NEWMAN had been smuggling in the narcotics into the prison. DENMARK took the narcotics from NEWMAN's home, stored them at his own residence and wished to turn them over to law enforcement the following day, May 3, 2018. On May 3, 2018 DENMARK voluntarily provided four glassine bags of narcotics to Your Affiant, SA Susan Keller and Lt. Fanelli. Unbeknownst to Your Affiant at the time, DENMARK had a sixty-one minute phone conversation with NEWMAN on the night of May 2, 2018 after speaking to Lt. Fanelli and Your Affiant. Your Affiant believes that DENMARK notified NEWMAN of the conversation with Internal Affairs and the FBI.

9. On May 11, 2018, DENMARK unsuccessfully attempted to make three recorded phone calls with NEWMAN in the presence of Your Affiant and SA Keller at 10:48am, 10:51am and 11:04am. Phone records show DENMARK had been in contact with NEWMAN via phone conversations and text messages numerous times a day, every day since May 3, including May 11, in which four text messages and 7 phone calls were made prior to the attempts to make a recorded phone call with NEWMAN. Upon the departure of Your Affiant and SA Keller, ten text messages were exchanged between DENMARK and NEWMAN beginning at 11:31am. Your Affiant believes that DENMARK forewarned NEWMAN of the attempt to record the phone call and not to answer the phone during this time period. Your Affiant further believes that DENMARK discussed the attempts to record a phone call with NEWMAN at this time.

10. DENMARK and NEWMAN remained in daily communication through May 22, 2018 in



which DENMARK again attempted to make a recorded phone call with NEWMAN. At 5:08pm DENMARK sent NEWMAN a text message. At 6:27 pm DENMARK unsuccessfully attempted to make a recorded phone call. At 7:06pm and 7:14pm NEWMAN made a 105 second and a 150 second phone call to DENMARK. Your Affiant believes that DENMARK again forewarned NEWMAN of the attempt to record the phone call and not to answer the phone during this time period.

11. June 19, 2018 at 3:37pm, DENMARK unsuccessfully attempted to make a recorded phone call with NEWMAN in the presence of Lt. Fanelli and Your Affiant. DENMARK stated he was unsure why she would not answer the phone and that they had not been in contact for two weeks. Phone records show that DENMARK and NEWMAN had exchanged phone calls and text messages numerous times a day every day since May 22, 2018, including 48, 35, 25 and 25 second phone calls as well as 3 text messages on June 19, 2018 prior to the unsuccessful attempt to make a recorded phone call. Your Affiant believes that DENMARK again forewarned NEWMAN of the attempt to record the phone call and not to answer the phone during this time period.

12. On June 20, 2018 at 3:44pm and 4:03pm, DENMARK unsuccessfully attempted to make a recorded phone call with NEWMAN in the presence of Your Affiant and SA Keller. Phone records show that DENMARK had called NEWMAN three times and texted NEWMAN four times prior to the unsuccessful attempt to record a phone call including a 33 minute phone call at 6:41am and four text messages to NEWMAN between 2:45pm and 2:49pm. DENMARK then had three phone calls with NEWMAN between 5:50pm and 10:30 pm including 15 and 20 minute phone calls. Your Affiant believes that DENMARK again forewarned NEWMAN of the attempt to record the phone call and not to answer the phone during this time period.

13. DENMARK claimed to have received a phone call from NEWMAN on June 22, 2018, using a telephone at the PDP, in which he confronted NEWMAN about narcotics. DENMARK stated that this alleged conversation initiated a series of text messages between DENMARK and NEWMAN in which they argue about narcotics and smuggling contraband into the PDP. DENMARK provided screenshots of these text messages to Your Affiant on July 2, 2018.

14. The below table includes examples of these text messages between DENMARK and NEWMAN. The conversations between DENMARK and NEWMAN included pertinent and non-pertinent information. The table below only includes pertinent excerpts of text messages that DENMARK sent NEWMAN.

June 23, 2018	"and you don't have to worry about them messing with u anymore I had to start an argument so I can let them see that you didn't do nothing"
June 23, 2018	I told u why I did it and this the last time I'm tell u I did it so they would stop fucking with u"
June 27, 2018	"I told u what I had to do to get them off u"

15. DENMARK alleged that the above comments were in reference to NEWMAN's supervisors at PDP, who were scrutinizing NEWMAN's work over a situation in which NEWMAN received a 5 day suspension. Your Affiant verified that NEWMAN did receive a 5 day suspension as a result of a disciplinary hearing on June 18, 2018. Your Affiant believes that DENMARK was actually referring to the FBI and Internal Affairs as well as the Prison's investigation into NEWMAN.

16. On July 19, 2018, DENMARK voluntarily provided his cellular telephone to Your Affiant and Lt. Fanelli for the purposes of extracting information related to communications with NEWMAN. Prior to providing the cellular telephone, DENMARK deleted all data related to



NEWMAN including text messages, phone calls and contact information. Your Affiant believes this was an attempt to conceal DENAMRK's communications with NEWMAN in which he forewarned her of the investigation into NEWMAN by the FBI and PDP.

17. Your Affiant submitted the narcotics received from DENMARK on May 3, 2018 to the DEA Northeast Laboratory for analysis. The DEA Northeast Laboratory established that the drug exhibit submitted was identified as Heroin Hydrochloride.

18. Your Affiant requested cellular telephone subscriber and toll information for NEWMAN's cellular telephone number, **513-283-3799**, and received this information from Sprint PCS. The telephone toll records provide law enforcement with the date, time, duration, call type, direction and other information regarding the incoming and outgoing calls on telephone number **513-283-3799**, but specifics, such as the content of text messages, are not provided.

19. Your Affiant requested cellular telephone subscriber and toll information for DENMARK's cellular telephone number, **215-390-7572** but has not received the records as of October 24, 2018.

20. In my training and experience, I have learned that Sprint PCS and T-Mobile USA, Inc., are companies that provide cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Sprint PCS and T-Mobile USA, Inc. subscribers may be located on the computers of Sprint PCS and T-Mobile USA, Inc. Further, I am aware that computers located at Sprint PCS and T-Mobile USA, Inc. contain information and other stored electronic communications belonging to unrelated third parties.

21. Wireless phone providers often provide their subscribers with voicemail services. In

general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Sprint PCS and T-Mobile USA, Inc. for a period of weeks to months, or longer.

22. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Sprint PCS and T-Mobile USA, Inc. for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

23. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

24. Wireless providers may also retain text messaging logs that include specific information



about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

25. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

26. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate

and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

27. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

28. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove the elements of the offenses being investigated, or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may



tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

29. Accordingly, the stored communications in the account for telephone numbers **513-283-3799** and **215-390-7572** (used by NEWMAN and DENMARK respectively) may provide direct evidence of the offenses under investigation. Based on my training and experience, text messages, telephone call logs, contact lists, voicemails, photos, videos, and documents (such as those stored on Sprint PCS and T-Mobile USA, Inc.'s servers) are often created and used in furtherance of criminal activity, including to communicate about and facilitate the offenses under investigation.

#### **ELECTRONIC DEVICES AND STORAGE**

30. As described above and in Attachment A and C, this application seeks permission to search and seize items and information that maybe stored in the Sprint PCS and T-Mobile USA, Inc. accounts for cellular telephone numbers **513-283-3799** and **215-390-7572** (used by NEWMAN and DENMARK respectively), in whatever form they are stored. Based on my experience and training, as well as the experience and training of other agents, I know that

electronic device accounts can store information for long periods of time. This information includes, voicemails, text messages, telephone contacts, phone logs and other media that may have been stored or downloaded to the cellular telephone account.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Sprint PCS and T-Mobile USA, Inc. to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in in Section I of Attachment B and D. Upon receipt of the information described in Section I of Attachment B and D, government-authorized persons will review that information to locate the items described in Section II of Attachment B and D.

**CONCLUSION**

32. Based on my training, experience, and the information contained in this affidavit, I submit that probable cause exists to believe that DANIEL DENMARK and MELANIE NEWMAN have committed violations of Title 18, United States Code, Section 1001(a)(2). I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities of such crimes may be found in the Sprint PCS and T-Mobile USA, Inc., accounts for cellular telephone numbers 513-283-3799 and 215-390-7572, used by NEWMAN and DENMARK respectively. Accordingly, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the cellular phones account described in Attachment A and C to seek the items described in Attachment B and D.

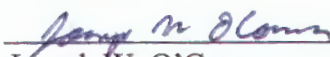


33. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).

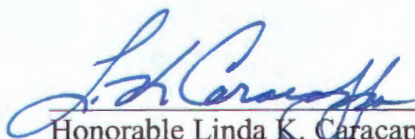
**REQUEST FOR SEALING**

34. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

  
\_\_\_\_\_  
Joseph W. O'Connor  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on Nov. 1, 2018, 2018

  
\_\_\_\_\_  
Honorable Linda K. Caracappa  
Chief, United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with a T-Mobile USA, Inc., cellular telephone account for cellular telephone number, **215-390-7572**, that is stored at premises owned, maintained, controlled, or operated by T- Mobile USA, Inc., a company headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by T-Mobile USA, Inc.:**

To the extent that the information described in Attachment A is within the possession, custody, or control of T-Mobile USA, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to T-Mobile USA, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), T-Mobile USA, Inc., is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from March 1, 2018 to present;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;
- e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names,

addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from March 1, 2018 to present;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from March 1, 2018 to present;

h. Incoming and outgoing telephone numbers, from March 1, 2018 to present;

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between T-Mobile USA, Inc. and any person regarding the account or identifier, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1001(a)(2), involving DANIEL DENMARK, MELANIE NEWMAN, and others yet unknown from March 1, 2018 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Drug trafficking;

b. Smuggling of contraband into prison;



- c. Discussions related to the investigations by the FBI and/or Philadelphia Department of Prisons into criminal activity committed by DANIEL DENMARK and/or MELANIE NEWMAN, to include any forewarnings of attempts to record phone calls.
- d. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- e. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- f. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- g. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- h. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the distribution of controlled substances and conspiracy to commit the same, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
BUSINESS RECORDS PURSUANT TO FEDERAL RULE  
OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by T-Mobile USA, Inc., and my official title is \_\_\_\_\_. I am a custodian of records for T-Mobile USA, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of T-Mobile USA, Inc., and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of T-Mobile USA, Inc.; and
- c. such records were made by T-Mobile USA, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature



**ATTACHMENT C**

**Property to Be Searched**

This warrant applies to information associated with a Sprint PCS, cellular telephone account for cellular telephone number, **513-283-3799**, that is stored at premises owned, maintained, controlled, or operated by Sprint PCS, a company headquartered at 6480 Sprint Parkway, Overland Park, KS 66251.

**ATTACHMENT D**

**Particular Things to be Seized**

**I. Information to be disclosed by Sprint PCS:**

To the extent that the information described in Attachment C is within the possession, custody, or control of Sprint PCS, including any messages, records, files, logs, or information that have been deleted but are still available to Sprint PCS, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Sprint PCS, is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment C:

k. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;

l. All existing printouts from original storage of all of the text messages described above;

m. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from March 1, 2018 to present;

n. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;

o. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names,



addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

p. Detailed billing records, showing all billable calls including outgoing digits, from March 1, 2018 to present;

q. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from March 1, 2018 to present;

r. Incoming and outgoing telephone numbers, from March 1, 2018 to present;

s. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

t. All records pertaining to communications between Sprint PCS and any person regarding the account or identifier, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1001(a)(2), involving MELANIE NEWMAN, DANIEL DENMARK, and others yet unknown from March 1, 2018 to present, including, for each account or identifier listed on Attachment C, information pertaining to the following matters:

i. Drug trafficking;

j. Smuggling of contraband into prison;

- k. Discussions related to the investigations by the FBI and/or Philadelphia Department of Prisons into criminal activity committed by DANIEL DENMARK or MELANIE NEWMAN, to include any forewarnings of attempts to record phone calls.
- l. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- m. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- n. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- o. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- p. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the distribution of controlled substances and conspiracy to commit the same, including records that help reveal their whereabouts.



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
BUSINESS RECORDS PURSUANT TO FEDERAL RULE  
OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Sprint PCS, and my official title is \_\_\_\_\_. I am a custodian of records for Sprint PCS. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Sprint PCS, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Sprint PCS; and
- c. such records were made by Sprint PCS as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature